

**PATENT****REMARKS**

Reconsideration of the rejections set forth in the Office action dated 7/6/2005 is respectfully requested under the provisions of 37 CFR §1.111(b).

Claims 1-3, 5-15 and 17-22 are pending.

Claims 1-3, 5-15 and 17-22 stand rejected.

Claims 1, 13 and 20 were amended. Claim 1 was amended to include the limitation that the server receive a performance specification for the cryptographic service and to perform that cryptographic service responsive to that specification. Independent claims 13 and 20 were similarly amended. Support for this limitation is found at least at page 22, lines 1-6.

Applicant petitions for a two month extension and authorizes the charging of the corresponding fee to Xerox Corporation Deposit Account No. 24-0025.

***I. Rejections under 35 USC 101***

Claim 20 was rejected as directed to non-statutory subject matter. Applicant respectfully traverses this rejection in light of the Precedential Opinion of Ex party Lundgren (Appeal No. 2003-2088) and further in light of the *Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility*. The application itself enables one of ordinary skill in the art to understand the utility of the invention of claim 20. The invention of claim 20 physically transforms an article or physical object to a different state or thing. In addition, invention of claim 20 produces a useful, concrete, and tangible result. Thus, applicant respectfully traverses this rejection to Claim 20.

***II. Rejections under 35 USC §103(a)***

Claims 1-3, 5-15 and 17-22 stand rejected under 35 USC §103 as being unpatentable over McGarvey (6,643,774) in view of Dolan (5,604,801). This rejection is respectfully traversed in view of the following arguments.

**PATENT**

A prima facie case of obviousness is established by one or more references that were available to the inventor and that teach a suggestion to combine or modify the reference, the combination or modification of which would appear to be sufficient to have made the claimed invention obvious to one of the ordinary skill in the art.

General Comments regarding the claimed invention:

The currently claimed invention is directed towards a **cryptographic service**. The cryptographic service is described at page 15, line 19 through page 16, line 4; page 19, lines 13-19; and page 20, lines 17-22 (as well as the application as a whole).

To summarize, a cryptographic service provider operates a server. The server provides cryptographic services to clients such that the client can off-load the computational burden related to a cryptographic operation from the client computer to the server that provides the service at a specified performance. One example of such a cryptographic service is that of encrypting data provided by the client (page 19, lines 27-31). Another example is that of performing modular exponentiation (page 16, lines 27-31). Thus, instead of a client computer performing the cryptographic operation, the client sends a request to a server that performs the requested cryptographic service for the client in accordance with a performance specification (page 22, lines 1-6).

The server thus provides a cryptographic service to a client computer such that the client computer can off-load the computational burden due to cryptographic operations from the client computer to the cryptographic server. The cryptographic operations performed by the server are those that could have been performed by the client.

The invention of currently amended claim 1 is directed to a networked server that provides a cryptographic service. The method includes the following steps.

- (a) identifying, by the server, a client utilizing the network;
- (b) generating a tunnel on the network using a first key;
- (c) receiving a second key at the server from the client utilizing the tunnel, wherein the second key is encrypted by the client using the first key, the second key being a private key of a key pair;

**PATENT**

- (d) receiving a performance specification for the cryptographic service;  
and
- (e) performing the cryptographic service at the server for the client, responsive to the performance specification, the server using the second key to perform the cryptographic service, whereby the server off-loads a computational burden associated with the cryptographic service from the client.

Thus, the invention of the currently amended claim 1 is directed to providing a cryptographic service from a networked server where the networked server receives a private key of a key pair over the tunnel and uses the private key to perform the cryptographic service in accordance with a performance specification, thus off-loading the computational burden associated with the cryptographic service from the client computer to the server computer.

McGarvey

**With regards to McGarvey:** McGarvey teaches techniques for allowing a server to use a client computer's (or user's) authority so that the server computer can access protected resources or perform protected services on behalf of the client (McGarvey column 2, lines 4-11; column 6, line 64 – column 7 line 16; and column 8, lines 52-56). McGarvey also teaches a public key system using public/private key pairs (column 1, line 56-column 2, line 11).

The problem addressed by McGarvey is how to allow a client computer to give a server the same access to protected data or services that the client has. It does this by delegating client authority to a server so that the server can access the protected data or services in place of the client. This delegation is accomplished by using a public key encryption system to establish trusted communication between a client, a server, and a private key system.

**PATENT**

Nothing in McGarvey teaches to one skilled in the art a suggestion to modify McGarvey to send the client's private key of a key pair and a performance specification to a server to perform the cryptographic service at the specified performance using the client's private key.

Dolan

**With regards to Dolan:** Dolan teaches a server that that provides cryptographic services to a client computer and that securely uses a client's key.

Nothing in Dolan teaches to one skilled in the art a suggestion to modify Dolan to send the client's private key of a key pair and a performance specification to a server to perform the cryptographic service at the specified performance using the client's private key.

Analysis

Nothing in McGarvey or Dolan, separately or combined, teaches to one skilled in the art a suggestion to modify either McGarvey or Dolan to send the client's private key of a key pair and a performance specification to a server to perform the cryptographic service at the specified performance using the client's private key.

Thus, currently amended **claim 1** is patentable. Currently amended **claim 13** and currently amended **claim 20** are a program product claim and a system claim (respectively) that are comparable with currently amended claim 1 and so are also patentable for the same reasons.

**Original claims 2 and 14** depend on and further limit their respective independent claims that are patentable and thus claims 2 and 14 are also patentable.

**Previously presented claims 3 and claim 15** depend on and further limit their respective parent claims that are patentable and thus claims 3 and 15 are also patentable.

**Previously presented claim 21** depends on and further limits patentable claim 3 and thus claim 21 is also patentable.

**PATENT**

**Previously presented claims 5 and 17** depend on and further limit their respective independent claims that are patentable and thus claims 5 and 17 are patentable. Furthermore, nothing in McGarvey or Kirby, separately or combined, teach a suggestion that would lead one skilled in the art to off-load modular exponentiation from a client to a cryptographic server.

**Previously presented claims 6 and 18** depend on and further limit their respective independent claims that are patentable. Thus claims 6 and 18 are also patentable.

**Original claim 22** depends on and further limits patentable claim 21 and thus claim 22 is also patentable.

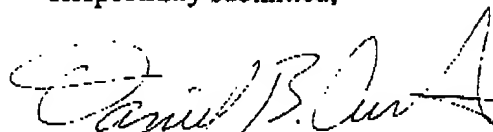
**Previously presented claims 7-9 and 19; and original claims 10-12** depend on and further limit their respective parental claims that are patentable. Thus, claims 7-9, 10-12 and 19 are patentable.

Since all rejections, objections and requirements contained in the outstanding official action have been fully answered or traversed and shown to be inapplicable to the present claims, it is respectfully submitted that reconsideration is now in order under the provisions of 37 CFR §1.111(b) and such reconsideration is respectfully requested. Upon reconsideration, it is also respectfully submitted that this application is in condition for allowance and such action is therefore respectfully requested.

**PATENT**

The undersigned Xerox Corporation attorney hereby authorizes the charging of any necessary fees, other than the issue fee, to Xerox Corporation Deposit Account No. 24-0025. This also constitutes a request for any needed extension of time and authorization to charge all fees therefor to Xerox Corporation Deposit Account No. 24-0025. Should any additional issues remain, or if I can be of any additional assistance, please do not hesitate to contact me at (650) 812-4259.

Respectfully submitted,



DANIEL B. CURTIS  
Attorney for Applicants  
Reg. No. 39,159  
(650) 812-4259  
dbcurtis@parc.com